IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

KIMBERLY DEKENIPP, *on behalf of herself and all individuals similarly situated*, Plaintiff, v. NATIONSBENEFITS, LLC, and FORTRA, LLC, Defendants.	Case No. _____ **TRIAL BY JURY DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kimberly Dekenipp, individually and on behalf of all others similarly situated, brings this action against NationsBenefits, LLC ("NationsBenefits") and Fortra, LLC ("Fortra"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

SUMMARY OF THE CASE

1. On April 13, 2023, NationsBenefits, a supplemental health benefits administration company disclosed that in late January 2023, it experienced a massive data breach, (the "Data Breach" or "Breach"), resulting in the disclosure and theft of over three million individuals' highly sensitive personal identifiable information ("PII") and health information ("protected health information" or "PHI"). Plaintiff Dekenipp's own PII and PHI was stolen in the Breach.

2. A cyber-criminal group called the "Clop ransomware gang" ("Clop"), a group of cyber criminals known for their attacks against the healthcare sector, took credit for exfiltrating vast troves of unencrypted, highly sensitive information from NationsBenefits' file transfer program, supplied by Fortra. Indeed, other cyber-criminal groups may also have taken advantage of this vulnerability along with Clop, increasing the severity of the Breach.

3. For years, NationsBenefits has directly and indirectly collected highly sensitive information from its own clients and the customers of its partner health insurance organizations.

4. As a result of the Data Breach, over three million people, including Plaintiff Dekenipp, had their PII and PHI compromised and sold on the dark web.

5. The Data Breach was a direct result of NationsBenefits' and Fortra's severely deficient cybersecurity practices, and the wealth of information and warnings available to Defendants makes their failures even more egregious.

6. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental part of doing business in the modern age— especially for businesses that profit from analyzing and processing PII and PHI. By collecting, maintaining, and profiting from Plaintiff's and the class members' PII and PHI, NationsBenefits and Fortra were required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information—and they failed to do so.

7. Among myriad industry standards and statutes setting the industry standards for protection of sensitive information, health care information is specifically protected by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like NationsBenefits to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

8. Instead, Defendants' woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of their negligence. Defendants disregarded the rights of Plaintiff and class members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard its customers' PII and PHI and by failing to take available and necessary steps to prevent unauthorized disclosure of that data.

9. The highly sensitive information exfiltrated in the Data Breach includes, but is not limited to, full names, dates of birth, social security numbers, phone numbers, addresses, gender, health plan subscriber identification numbers, and Medicare numbers.

10. Even though it was Defendants' dereliction of duty that led to the Data Brach, it is Plaintiff Dekenipp, and the other victims of the Data Breach that will bear the burden of Defendants' negligence for years to come.

11. The exponential cost to Plaintiff Dekenipp and the class members resulting from the Data Breach cannot be overstated. Criminals can use victims' names, birth dates, social security numbers, and addresses to open new financial accounts, incur charges in credit, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it.[1] Any one of these instances of identity theft can have devastating consequences for the victim— causing years of often irreversible damage to their credit scores, financial stability, and personal security.

12. Likewise, the exfiltration of the PHI puts Plaintiff and the class members at imminent risk for medical identity theft, especially in light of the high demand and value of Medicare identification numbers on the dark web.[2] Medical identity theft poses an even more critical threat to victims—medical fraud could lead to loss of access to

---

[1] *See, e.g.*, *Report to Congressional Requesters*, United States Government Accountability Office (June 2007), http://www.gao.gov/assets/270/262899.pdf; Melanie Lockert, *How do hackers use your information for identity theft?*, CreditKarma (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information; Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2020), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LifeLock by Norton (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft.

[2] *What to Know About Medical Identity Theft*, Federal Trade Commission (May 2021), https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

necessary healthcare if through misuse of paid-for insurance benefits or by incurring substantial medical debt.

13. Due to the highly valuable nature of PHI, the FBI has even warned healthcare providers that they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.[3]

14. Plaintiff and the class are at imminent, certain risk for identity theft because of the nature of the PII and PHI exposed.

15. NationsBenefits and Fortra's impermissibly lax data security practices resulted in Plaintiff and the class members becoming imminently at risk for identity or medical identity theft, but NationsBenefits maximized the harm inflicted by waiting more than two months before notifying its effected customers that their highly sensitive, private information was stolen by and in the hands of sophisticated cyber criminals.

16. Although NationsBenefits first began notifying class members of the breach on April 13, 2023, it did not provide Plaintiff Dekenipp with notice until April 27, 2023, which prevented her from taking immediate defensive measures to protect her valuable PII and PHI.

---

[3] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820, (last visited June 6, 2023).

17. Plaintiff Dekenipp and class members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) lost value of PII/PHI, a form of property that Defendants obtained from Plaintiff and class members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII/PHI; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain risk that unauthorized persons will access and abuse Plaintiff's and class members' highly sensitive PII/PHI that is available on the dark web; (v) the continued and certain increased risk that the PII/PHI that remains in Defendants' possession is subject to further unauthorized disclosure for so long as Defendants fail to undertake proper measures to protect the PII; and (vi) theft of their PII/PHI and the resulting loss of privacy rights in that information.

18. As a direct and proximate result of the Data Breach and Defendants' failure to protect Plaintiff Dekenipp's and the class members' unencrypted PII/PHI, Plaintiff and the class members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, social engineering, and other misuses of their PII/PHI, as well as an increased risk to their personal safety; ongoing monetary loss and economic harm, including loss of value of their PII/PHI; loss of value of privacy and confidentiality of the stolen PII/PHI; illegal sales of the compromised PII/PHI; mitigation expenses and time spent on credit monitoring;

identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiff Dekenipp and class members have a continuing interest in ensuring that their PII and PHI are and remains safe, and they should be entitled to injunctive and other equitable relief.

19. Finally, malicious actors will often wait months, or even years, to use stolen PII/PHI to lower chances of detection by the victim or temporary credit monitoring assistance. This means that Plaintiff or the class members could be victims of multiple instances of identity theft as a result of this single Data Breach. While Plaintiff and the class members are already at imminent risk for identity and medical identity theft, such risk will continue, possibly indefinitely, as a direct and foreseeable result of Defendants' negligence.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

21. This Court has personal jurisdiction over NationsBenefits. Upon information and belief, this limited liability company's sole member, Glenn Parker, resides in Fort Lauderdale, Florida, and is a citizen of Florida. NationsBenefits' headquarters and principal place of business is in Plantation, Florida.

22. This Court also has personal jurisdiction over Fortra pursuant to Florida's long-arm statute, Fla. Stat. § 48.193 (2017). Upon information and belief, this limited liability company's sole member, Matthew Reck, is a resident of Minnesota. Fortra's headquarters and principal place of business is in Eden Prairie, Minnesota. Fortra "engag[es] in … business," and has committed "tortious acts" within Florida. *See* Fla. Stat. § 48.193(1)(a)(1)–(2).

23. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and NationsBenefits and Fortra conduct substantial business in this District.

DEFENDANTS

24. NationsBenefits provides supplemental benefits administration services to employers, health insurance companies, and other entities' health plans. It is headquartered in Plantation, Florida, and serves "millions" of members as a "leading provider of supplemental benefits, flex cards, and member engagement solutions that

partners with managed care organizations to provide innovative healthcare solutions designed to drive growth, improve outcomes, reduce costs, and delight members."[4]

25. Fortra is a cybersecurity software and services company based in Eden Prairie, Minnesota. Among its many products, Fortra is well known for its Managed File Transfer Service ("GoAnywhere MFT") which enables its clients to securely share files internally and with external organizations.

NAMED PLAINTIFF

26. Plaintiff Kimberly Dekenipp is a resident and citizen of Alvin, Texas. Upon information and belief, NationsBenefits acquired her PII/PHI from her insurance provider, Aetna. Prior to the Data Breach, Plaintiff took reasonable steps to keep her PII/PHI confidential and secure. Following the Data Breach, where Plaintiff's PII/PHI, including her social security number, was exfiltrated, Plaintiff has spent considerable time and effort regularly monitoring her accounts to detect fraudulent activity in order to mitigate against potential harm, especially because the leak of her highly sensitive information means that she is substantially at risk for identity theft or medical identity theft in the future. With her highly sensitive information now available for any nefarious actor to purchase online, Plaintiff is at a substantial and imminent risk of future harm, including but not limited to identity theft and medical identity theft.

FACTUAL ALLEGATIONS

[4] *See* NationsBenefits, *About Us*, https://www.nationsbenefits.com/about-us (last visited June 5, 2023).

A. NationsBenefits' Collection and Use of Customer Data

27. NationsBenefits is one of the fastest-growing supplemental benefits administration companies in the United States, which provides its services to health insurance plans and employers across the country. Founded in 2015 as "Nation's Hearing," NationsBenefits now provides an array of supplemental healthcare solutions, including:

a. NationsHearing, which provides hearing benefits, such as digital hearing tests, annual hearing tests, and coverage for hearing aids or related technologies;

b. NationsOTC, which provides benefits administration and an e-commerce platform for over-the-counter health items, such as foods, first-aid supplies, and other health and wellness items;[5]

c. NationsMarket, which provides benefits administration for purchasing healthy foods, including prepared meals, fresh produce, and groceries;

d. NationsCare, which is a companion care benefit, which provides a Companion to members for non-medical assistance such as emotional support, household chores, errands, and transportation;[6]

---

[5] *See* NationsBenefits, *NationsOTC*, https://www.nationsbenefits.com/nationsotc (last visited June 5, 2023).

[6] *See* NationsBenefits, *Optimized Companion Care Benefit*, https://www.nationsbenefits.com/Wellness#optimizedcompanioncarebenefit (last visited June 5, 2023).

e. A Personal Emergency Response Systems benefit, which includes in-home Medical Alert base units, help buttons, GPS monitoring, and other monitoring for elderly members;[7] and

f. Connectivity devices, such as tablets, fitness trackers, and phones, for elderly members.[8]

28. It also provides customer experience services for insurance plans, leveraging data analytics to increase member engagement and satisfaction.[9]

29. By virtue of its partnerships with other healthcare organizations, NationsBenefits collects and processes an enormous volume of personal data from millions of individuals, including personal information, health and patient records and insurance information, geolocation data, and financial information. Much of this information is not provided to NationsBenefits by the individuals themselves, but by their insurance providers or employers.

30. NationsBenefits strongly urges—or even requires—its clients, users, and patients to provide PII/PHI to leverage any of its products and services.

---

[7] *See* NationsBenefits, *Wellness Solutions*, https://www.nationsbenefits.com/Wellness#pers-benefit (last visited June 5, 2023).

[8] *See id.*

[9] *See* NationsBenefits, *NationsCX*, https://www.nationsbenefits.com/NationsCX (last visited June 5, 2023).

NationsBenefits explicitly warns customers that certain services "may require you to provide personal information."[10]

31. One method of direct information collection occurs on its membership platform, the MyBenefits Portal, where members fill out a personal health profile, including sensitive information about current health concerns, and can purchase goods and services with their supplemental benefits. Members can also schedule appointments with recommended doctors through this platform and share medical records with providers.

32. Upon information and belief, NationsBenefits also receives and maintains the PHI of the patients and employees of its partners, including individuals' names, addresses, dates of birth, member identification numbers, date of health plan coverage, and social security numbers.

33. NationsBenefits routinely collects PII, including payment card information, billing and shipping information, location information, and purchase histories.[11] It collects this information from its members profiles, transactions, interactions with its services, and its partnerships with health plans and employers.

34. NationsBenefits admits to collecting, storing, and analyzing all of this highly sensitive information—in fact, it touts its use of data and analytics as a

---

[10] *See* NationsBenefits, *Privacy Policy*, https://nationsbenefits.com/privacy (last visited June 5, 2023).

[11] *Id.*

cornerstone of its product line.[12] NationsBenefits maintains and mines the data for product development, targeted solicitation for new products and referrals to existing partnerships, and target marketing of new partners—all in an effort to boost its profits.

35. To distinguish itself from other competitors in the supplemental benefits market, NationsBenefits highlights its data collection and analytics, including analyzing past and present clinical health plan data to "assess known and unknown member needs."

36. Even though some individuals may not use NationsBenefits' services directly, NationsBenefits still collects, maintains, and profits from their data that is shared from their insurance providers or employers. These individuals have no choice in sharing this information and have no control over how NationsBenefits protects—or fails to protect—their sensitive, personal information.

37. NationsBenefits acquired, stored, collected, and represented that it maintained reasonable security over Plaintiff's and the class members' PII/PHI.

38. By taking and collecting Plaintiff and the class members' sensitive information, NationsBenefits agreed to use reasonable safety and security measures in line with industry standards.

---

[12] *See* NationsBenefits, *Outcomes-based Approach*, https://www.nationsbenefits.com/outcomes (last visited June 6, 2023).

39. By obtaining, collecting, receiving, and/or storing Plaintiff's and class members' PII/PHI NationsBenefits assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and class members' PII/PHI from unauthorized disclosure.

40. In its Privacy Policy, NationsBenefits promises customers that it will "use reasonable physical, technical, and administrative safeguards" to protect customers PII/PHI.[13]

41. It also promises customers that it will only share customer information in limited circumstances, none of which include sharing with the cyber criminals that facilitated the Data Breach.[14]

B. NationsBenefits Partners with Fortra for Secure File Transfer Services and Data Storage.

42. To facilitate sharing of sensitive patient information between NationsBenefits, its insurance provider and employer clients, and healthcare providers, NationsBenefits purchased and used a managed file transfer software from Fortra: the GoAnywhere MFT.

43. Fortra bills itself as "a positive changemaker for cybersecurity" that is "dedicated to building leading solutions and adapting to stay ahead of the ever-evolving

[13] *See* NationsBenefits, *Privacy Policy*, *supra* n.10.

[14] *Id.*

threat landscape."[15] As a cybersecurity company with products including vulnerability management, email security, phishing protection, data protection, among others, Fortra markets itself as an expert in data security and protection.[16]

44. The GoAnywhere MFT "is a managed file transfer solution that automates and secures file transfers using a centralized enterprise-level approach."[17] It acts as a "central point of administration" between an organization's internal organization, external partners and clients, appliances, and cloud environments.[18] It allegedly includes "extensive security controls" and "automatic encryption" that may be customized for each organization.[19] Fortra promised that the GoAnywhere MFT "will provide a safe, audited method for automatically transferring information in and outside of your enterprise."[20]

45. Despite these promises, on information and belief, the default settings for the GoAnywhere MFT are not compliant with reasonable security standards. The

---

[15] Fortra, *Meet Fortra*, https://www.fortra.com/about (last visited June 6, 2023).

[16] Fortra, *Cybersecurity & Automation Solutions*, https://www.fortra.com/solutions#securityservices (last visited June 6, 2023).

[17] Fortra, *Start Using GoAnywhere MFT*, https://www.goanywhere.com/offers/start-using-mft (last visited June 6, 2023).

[18] *Id.*

[19] *Id.*

[20] *Id.*

GoAnywhere MFT installation guide provides instructions for how to make the product more secure.

46. For example, the default configuration of the GoAnywhere MFT allows anyone with access to the internet to view the landing page, or "administrative console" for a client's GoAnywhere MFT, where users can sign in to access, operate, and modify the program.[21] Fortra's instructions provide several simple steps that limit public access to this console, such as limiting access to specific ports, meaning that only certain users can access an organization's administrative console. Without these changes, the GoAnywhere MFT is vulnerable to attack and exploitation, and is not compliant with reasonable security standards and HIPAA requirements.[22]

47. Fortra has also disclosed security vulnerabilities in the GoAnywhere MFT in the past, which rendered their software vulnerable to exploitation.[23]

48. On information and belief, NationsBenefits and Fortra jointly controlled the security and configurations of the MFT servers that stored sensitive information for

---

[21] Fortra, *GoAnywhere MFT Install Guide*, https://static.goanywhere.com/guides/ga_installation_guide.pdf.

[22] Dave Shackleford, *Web-Based Admin Consoles: The Critical, Overlooked Security Exposure you must Address*, BeyondTrust (Aug. 10, 2021), https://www.beyondtrust.com/blog/entry/web-based-admin-consoles-the-critical-overlooked-security-exposure-you-must-address.

[23] Fortra, *GoAnywhere MFT Security Advisory*, https://www.goanywhere.com/support/advisory/68x.

transfer, and were responsible for protecting, maintaining, and monitoring those servers for threat activity.

49. On information and belief, NationsBenefits and/or Fortra did not update the default settings on NationsBenefits' installation of the GoAnywhere MFT, including leaving the administrative console exposed to anyone with internet access, failing to comply with reasonable security standards and HIPAA requirements.

C. The Data Breach

50. Between January 18, 2023, and January 30, 2023, Clop accessed NationsBenefits servers through a vulnerability in the GoAnywhere MFT administrative console.

51. Over 130 organizations, including several healthcare organizations, were affected by data breaches stemming from this attack.[24]

52. Despite the fact that similar vulnerabilities in administrative consoles are a common method of exploitation, the developers and administrators did not prevent the attack.

53. This vulnerability, assigned the number CVE-2023-0669 by the National Institute of Standards and Techology ("NIST"), is only accessible to attackers where

[24] Danny Wimmer, Fortra Data Breach Targets 130 Companies, Many in Healthcare Sector, Michigan Department of Attorney General (May 16, 2023), https://www.michigan.gov/ag/news/press-releases/2023/05/16/fortra-data-breach-targets-130-companies-many-in-healthcare-sector.

the GoAnywhere MFT administrator console is publicly accessible through the internet, as was the case with NationsBenefits' MFT.[25]

54. The vulnerability allowed the hackers to take the following actions on Defendants' servers:

a. Create unauthorized user accounts and download files from MFT servers; and

b. Install two tools, "Netcat"[26] and "Errors.jsp"[27] which enabled the hackers to exfiltrate data and establish "backdoors" into the breached system, which allow them to access more data and re-enter the breached systems at later dates.

55. Upon information and belief, these actions enabled the hackers not only to access and download Defendants' customers' sensitive personal information, but

---

[25] Caitlin Condon, *Exploitation of GOAnywhere MFT zero-day vulnerability*, Rapid7 (May 4, 2023), https://www.rapid7.com/blog/post/2023/02/03/exploitation-of-goanywhere-mft-zero-day-vulnerability.

[26] Bill Toulas, *Fortra shares findings on GoAnywhere MFT zero-day attacks*, BleepingComputer (April 19, 2023), https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/ (Netcat is "is a versatile networking utility that threat actors typically use to establish backdoors, conduct port scanning, or transfer files between the compromised system and their server.").

[27] *Id.* ("Errors.jsp is a JavaServer Pages (JSP) file used for creating dynamic web pages. Fortra does not explain how the attackers used the file. However, it's possible that it was designed to provide the attacker with a web-based backdoor on the breached system for executing commands, stealing data, or maintaining access to the environment.").

also to move across Defendants' other networks and systems to access vast troves of personal information.

56. Upon information and belief, Clop issued a ransom demand to NationsBenefits and threatened to leak customer data unless paid. The hackers claimed to have acquired "Customer databases: name, address, phone number, date of birth, gender, marital status, insurance company name and address. [L]ogs and backups of the production server," and released the data in five parts.[28]

57. Upon information and belief, Clop has already posted and/or sold Plaintiff and the class members' sensitive information on their dark web-based store, known as "Clop Leaks."[29]

58. In a statement, the hackers claimed that they could access other parts of victim's networks and systems and deploy malware, "but decided against it and only stole the documents stored on the compromised GoAnywhere MFT servers."[30]

---

[28] Databreaches.net, *The Fortra/GoAnywhere breach also affected healthcare entities. Here's what we know so far*, (April 21, 2023), https://www.databreaches.net/the-fortra-goanywhere-breach-also-affected-healthcare-entities-heres-what-we-know-so-far/

[29] *Id.*

[30] Sergui Gatlan, *Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day*, BleepingComputer (Feb. 10, 2023), https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day.

59. Other cyber-criminal groups and attackers leveraged this exploitation alongside Clop, making the true impact and scale of the leak unknown.[31]

60. Upon information and belief, Plaintiff's and the class members' PII/PHI was unprotected and unencrypted, and therefore easily accessible for unauthorized access and exfiltration.

61. Although NationsBenefits was compromised on January 30, it did not recognize that its servers had been hacked for at least nine more days.[32] And even though Fortra notified its customers of the exploit on February 3, 2023, NationsBenefits did not take steps to secure their servers until much later.

62. Indeed, the length of time the Data Breach went unnoticed and undetected by Defendants is astonishing. Fortra notified enterprise customers of the exploit on February 3, 2023, providing details of the exploit, indicators of compromise, and mitigation options.[33] Security researchers and news outlets quickly disseminated the

---

[31] Ido Lev, *BlackCat / Alphv Ransomware Group Exploits GoAnywhere Vulnerability (CVE-2023-0669) With Higher-Than-Average Demands*, At Bay (Apr. 25, 2023), https://www.at-bay.com/articles/blackcat-ransomware-group-exploits-goanywhere-vulnerability.

[32] Steve Adler, *NationsBenefits Holdings Confirms 3 Million Record Data Breach*, The HIPAA Journal (May 8, 2023), https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach.

[33] Sergui Gatlan, *Exploit released for actively exploited GoAnywhere MFT zero-day*, BleepingComputer (Feb. 6, 2023), https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-exploited-goanywhere-mft-zero-day.

warning en masse. As of February 4, 2023, media outlets Security Affairs and the Hacker News released detailed articles detailing that the exploits were being leveraged by malicious actors and providing potential mitigation steps that companies could take to prevent exploitation.[34]

63. Upon information and belief, NationsBenefits failed to update its systems to include the indicators of compromise or make any mitigation efforts until February 7, 2023, leaving their systems unprotected and open for exploitation for over a week.

64. NationsBenefits waited more than two months after it discovered its customers' PII/PHI had been stolen before sending notices to individuals whose data was stolen in the Breach. While NationsBenefits first sent notices to impacted individuals on April 13, 2023, Plaintiff's letter was not sent until April 27, 2023. The notice stated the following:

> **What Happened?** NationsBenefits used software provided by a third-party vendor, Fortra, LLC ("Fortra"), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our

[34] *See* Pierluigi Paganini, *GoAnywhere MFT zero-day flaw actively exploited*, Security Affairs (Feb. 4, 2023), https://securityaffairs.com/141826/hacking/goanywhere-mft-zero-day.html (last visited June 6, 2023); Ravie Lakshmanan, *Warning: Hackers Actively Exploiting Zero-Day in Fortra's GoAnywhere MFT*, The Hacker News (Feb. 4, 2023), https://thehackernews.com/2023/02/warning-hackers-actively-exploiting.html (last visited June 6, 2023).

> investigation, NationsBenefits analyzed the impacted data to determine whether any individual's personal information was subject to unauthorized access or acquisition. On February 23, 2023, NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.
>
> **What Information Was Involved?** The personal information involved included your First Name; Middle Initial; Last Name; Gender; Health Plan Subscriber Identification Number; Address; Date of Birth; Medicare Number.

65. Puzzlingly, Defendant NationsBenefits did not mention that the Clop hackers very likely stole even more information from Defendants' systems, including: social security numbers, full names, and phone numbers. Given the sensitive information stored on NationsBenefits' servers, other data that may have been accessed and stolen includes medical records, financial information, and geolocation information. Due to the high level of access that the attackers had into the Defendants' servers, this additional information was likely exposed for exfiltration and stolen.

66. On April 13, 2023, more than two months after it discovered the theft of its customers' highly sensitive information, NationsBenefits notified the United States Department of Health and Human Services that 3,037,303 individuals were affected by the Data Breach.[35]

[35] U.S. Department of Heath and Human Services, *Cases Currently Under Investigations*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last visited June 6, 2023).

D. Defendants' Knowledge of Cyber Security Threats

67. At all relevant times, Defendants were well aware, or reasonably should have been aware, that the PII/PHI collected, maintained, and stored in their servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, medical identity theft, fraud and other misuse.

68. File transfer services like GoAnywhere MFT are popular and well-known targets for cyberattacks. Some of the largest healthcare data breaches in recent history occurred by cyber criminals targeting file transfer services. For example, in February 2021, the file transfer service Accellion was attacked by the same threat actors as the Data Breach—Clop—causing the loss of more than three million patients' information.[36]

69. Indeed, Defendants knew or should have known that third-party vendors like Fortra were responsible for ninety percent of healthcare-related cyberattacks in 2021 and 2022.[37]

---

[36] Ionut Ilascu, Global Accellion data breaches linked to Clop ransomware gang, BleepingComputer (Feb. 22, 2021), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/; Cybersecurity Infrastructure & Security Agency, *Exploitation of Accellion File Transfer Appliance*, (June 17, 2021), https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-055a.

[37] Jessica Davis, *Most of the 10 largest healthcare data breaches in 2022 are tied to vendors*, SC Media (Dec. 12, 2022), https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors; Jessica Davis, *Vendor incidents lead the 10 biggest health care data breaches of 2021 so far*, SC Media (June 30, 2021), *(cont.)*

70. The frequency and prevalence of attacks make it imperative for entities to routinely and constantly monitor for exploits and attacks, and regularly update their software and security procedures.

71. NationsBenefits and Fortra were fully aware that the healthcare benefits industry is a prime target for cyber threats.[38] High profile data breaches in for similar industry leaders in healthcare put them on notice of this fact, *e.g.*, Trinity Health (3.3 million patients, May 2020); Shields Healthcare Group (2 million patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%, making it the fifth most common industry targeted by cyberattacks.[39]

72. Defendants also knew or should have known of the threat that Clop posed to their patients. The healthcare industry is also the primary target of Clop.[40] The Department of Health and Human Services even issued alerts in 2021 and early January

https://www.scmagazine.com/news/risk-management/vendor-incidents-lead-the-10-biggest-health-care-data-breaches-of-2021-so-far.

[38] *See* Finkle, *FBI warns healthcare firms they are targeted by hackers*, *supra* n.3.

[39] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year.

[40] HC3, *Analyst Note: Clop Ransomware*, HHS (Jan. 4, 2023), https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf.

2023 warning the healthcare sector of potential attacks from this hacking group.[41] Clop has previously targeted file transfer services as a means to target the healthcare sector.[42]

E. Defendants Breached Their Duties to Plaintiff

73. As entities collecting, maintaining, and profiting off of Plaintiff's and the class members' highly sensitive personal information, NationsBenefits and Fortra had a duty to exercise reasonable care and comply with applicable industry standards and statutory security requirements to protect their information.

74. NationsBenefits' HIPAA Rights disclosure even provides that they "are required by law to maintain the privacy and security of your protected health information."[43]

75. In its Privacy Policy, Fortra acknowledges that it may receive personal information from third party sources, including business partners and affiliates. It states that it "secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use, or disclosure."[44]

---

[41] *Id.*

[42] HC3, *Analyst Note: CLOP Poses Ongoing Risk to HPH Organizations*, HHS (Mar. 23, 2021), https://www.hhs.gov/sites/default/files/clop-poses-ongoing-risk-to-hph-organizations.pdf.

[43] NationsBenefits, *Your HIPAA Rights*, https://www.nationsbenefits.com/hipaa (last visited June 6, 2023).

[44] *See* NationsBenefits, *Privacy Policy*, *supra* n.10.

76. Despite holding PII/PHI for millions of individuals, NationsBenefits and Fortra failed to adopt reasonable data security measures to prevent and detect unauthorized access to their highly sensitive databases, putting their customers' highly sensitive information at risk.

77. NationsBenefits had the resources to prevent a breach and made significant expenditures to market their supplemental benefits and technology solutions, but neglected to invest adequately in data security, despite the growing number of well-publicized data breaches affecting the healthcare and insurance industries.

78. Defendants failed to properly implement data security practices that were reasonable and up to industry standards.

79. Upon information and belief, Defendants were at all times aware of their obligations and duties to protect Plaintiff's and class members' private information, and aware of the significant repercussions resulting from their failure to do so.

F. Defendants Failed to Comply with Regulatory Requirements and Industry Practices

80. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of PII/PHI.

81. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personal information, or PII, about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect PII/PHI from unauthorized access. Florida is one such state and requires that entities like Defendants "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. Ann. § 501.171(2).

82. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[45]

83. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[46] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII/PHI that is no longer needed; encrypt information stored on computer networks; understand their network's

---

[45] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 2, 2020).

[46] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.ov/system/files/documents/plain-language/pdf-0136_proteting-personal- information.pdf (last visited March 2, 2020).

vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

84. The FTC also recommends that companies not maintain PII/PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[47]

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC

---

[47] *See* FTC, *Start With Security*, *supra* n.46.

recognizes that failure to restrict access to information[48] and failure to segregate access to information[49] may violate the FTC Act.

87. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (i.e., PII/PHI) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

88. Furthermore, Defendants are required to comply with the HIPAA Privacy Rules and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set the nationwide standards for protecting health information, including health information stored electronically.

89. The Security Rule requires Defendants to do the following:

---

[48] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), available at https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

[49] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use "readily available security measures to limit access between" data storage systems).

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[50]

90. Pursuant to HIPAA's mandate that Defendants follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, Defendants were required to, at minimum, to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

[50] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited June 6, 2023).

91. Defendants are also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

92. Both HIPAA and HITECH obligate Defendants to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient PII. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. §17902.

G. The Effect of the Data Breach on Impacted Customers

93. Defendants' failure to keep Plaintiff's and class members' PII/PHI secure has severe ramifications. Given the sensitive nature of the information stolen in the Data Breach—names, social security numbers, birthdates, addresses, health information—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

94. The data exposed in the Data Breach, including customers' social security numbers, full names, dates of birth, and health insurance information, is highly coveted and valuable on underground or black markets. Upon information and belief, Plaintiff's and the class members' data has already been leaked and sold on the black market.

95. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs,

submit false bills to insurance companies, or even undergo surgery under a false identity.[51] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers, health insurance information, or social security numbers.

96. Medicare beneficiary numbers like Plaintiff's are "even more valuable than stolen credit cards," and often result in the filing of false claims for Medicare reimbursement.[52]

97. According to the U.S. Government Accountability Office, "stolen data may be held for up to a year or more before being used to commit identity theft," and "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[53]

98. Because of its value and the loss of sensitive health information and social security numbers, future identity theft is imminently and certainly impending.

---

[51] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited June 6, 2023).

[52] Melissa D. Berry, *Medicare under attack: Healthcare data breaches increase fraud risks*, Thomson Reuters (Mar. 3, 2023), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/medicare-fraud-risks.

[53] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTSGAO-07-737.htm (last visited June 5, 2023).

99. Identity thieves can use PII/PHI such as that exposed in the Data Breach to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

100. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[54]

101. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[55]

102. For Plaintiff and class members who had their social security numbers exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, social security numbers cannot easily be replaced. In order to obtain a new

---

[54] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era- complexity (last visited March 2, 2020).

[55] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited March 2, 2019).

number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[56]

103. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a social security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After

[56] Social Security Administration, *Identity Theft and Your Social Security Number*, available at http://www.ssa.gov/pubs/10064.html (last visited March 2, 2020).

conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

104. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[57] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower- interest loan.

105. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

106. The 2017 Identity Theft Resource Center survey[58] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety

---

[57] *Identity Theft: The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited June 6, 2023).

[58] *Id.*

- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

107. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[59]

[59] *Id.*

108. There may also be a significant time lag between when PII/PHI is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[60]

109. As the result of the Data Breach, Plaintiff and class members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- losing the inherent value of their PII/PHI;
- losing the value of NationsBenefits' implicit promises of adequate data security;
- identity theft and fraud resulting from the theft of their PII/PHI;
- costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;

[60] *See,* GAO, *Report to Congressional Requesters*, *supra* n.1.

- costs associated with purchasing credit monitoring and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being in the possession of one or many unauthorized third parties.

110. Additionally, Plaintiff and class members place significant value in data security.

111. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like NationsBenefits or Fortra would have no reason to tout their data security efforts to their actual and potential customers.

112. Consequently, had consumers known the truth about Defendants' data security practices—that Defendants would not adequately protect and store their data—they would not have entrusted their PII/PHI to NationsBenefits, purchased health benefits that included NationsBenefits' or Fortra's services, or paid as much for such services or benefits. As such, Plaintiff and class members did not receive the benefit of their bargain with NationsBenefits because they paid for a value of services they expected but did not receive.

CLASS ACTION ALLEGATIONS

113. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seek certification of the following nationwide class (the "Class" or the "Nationwide Class"):

All persons in the United States whose PII/PHI were compromised in the Data Breach.

114. The Nationwide Class asserts claims against all Defendants for negligence (Count 1), negligence *per se* (Count 2), and declaratory judgment (Count 3), and breach of the Florida Deceptive and Unfair Trade Practices Act (Count 6), and against NationsBenefits only for breach of implied contract (Count 4) and unjust enrichment (Count 5).

115. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seek certification of a Texas subclass (the "Texas Subclass") for statutory claims under Texas consumer protection statutes (Counts 7), defined as follows:

All persons in Texas whose PII/PHI were compromised in the Data Breach.

116. Excluded from the Nationwide Class and each State Subclass are Defendants, any entity in which any Defendants has a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each State Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

117. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

118. Each of the proposed classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

119. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Nationwide Class and Texas Subclass are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiff at this time, NationsBenefits has acknowledged that the PII/PHI of approximately 3,037,303 individuals throughout the United States was compromised in the Data Breach. Those persons' names and addresses are available from NationsBenefits' records and in data maintained by Fortra, and class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice.

120. **Predominance of Common Issues**. Fed. R. Civ. P. 23(a)(2) and (b)(3). Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include:

a. Whether Defendants knew or should have known that their GoAnywhere MFT servers and configurations were vulnerable to attack;

b. Whether Defendants failed to take adequate and reasonable measures to ensure that their computer, applications, and data systems were protected;

c. Whether Defendants failed to take available steps to prevent and stop the Breach from happening;

d. Whether Defendants owed tort duties to Plaintiff and class members to protect their PII/PHI;

e. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and class members;

f. Whether Defendants breached their duties to protect the PII/PHI of Plaintiff and class members by failing to provide adequate data security;

g. Whether Defendants' failure to secure Plaintiff's and class member's PII/PHI in the manner alleged violated federal, state and local laws, or industry standards;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiff's and class members' PII/PHI;

i. Whether NationsBenefits has an implied contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

j. Whether Defendants' conduct amounted to violations of state consumer protection statutes;

k. Whether, as a result of Defendants' conduct, Plaintiff and class members face a significant threat of identity theft, harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

l. Whether NationsBenefits should retain the money paid by Plaintiff and class members to protect their PII/PHI;

m. Whether Defendants should retain Plaintiff' and class members' valuable PII/PHI;

n. Whether, as a result of Defendants' conduct, Plaintiff and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

121. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Nationwide Class and the Texas Subclass, Plaintiff's claims are typical of other class members' claims because Plaintiff and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

122. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the classes and are committed to pursuing this matter against Defendants to obtain relief for the classes. Plaintiff has no conflicts of interest with the classes. Plaintiff's Lead Counsel are competent and experienced in litigating class actions, including extensive

experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of all of the classes.

123. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiff and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

124. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Each Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the classes as a whole, making injunctive and declaratory relief appropriate to the classes as a whole.

125. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

126. Finally, all members of the proposed classes are readily ascertainable. NationsBenefits has access to information regarding which individuals were affected by the Data Breach, and has already provided notifications. Using this information, the members of the classes can be identified, and their contact information ascertained for purposes of providing notice to the classes.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AND TEXAS SUBCLASS

COUNT 1
NEGLIGENCE
Against all Defendants

127. Plaintiff repeats and alleges Paragraphs 1–126, as if fully alleged herein.

128. NationsBenefits acquired, maintained, and profited from Plaintiff's and class members' sensitive personal information, including their social security numbers and Medicare numbers. NationsBenefits used Fortra's GoAnywhere MFT and other computing platforms to store and transfer this vast treasure trove of PII/PHI.

129. By collecting, storing, using, and profiting from this data, NationsBenefits and Fortra had a duty of care to Plaintiff and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by

unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing its security systems and data storage architecture to ensure that Plaintiff's and class members' PII/PHI was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely manner; (c) timely acting upon all warnings and alerts—including public information—regarding security vulnerabilities and potential compromises of the compiled data of Plaintiff and millions of class members; and (d) maintaining data security measures consistent with industry standards.

130. NationsBenefits and Fortra had common law duties to prevent foreseeable harm to Plaintiff and class members. These duties existed because Plaintiff and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and class members would be harmed by the failure to protect their PII/PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants also knew that it was more likely than not Plaintiff and other class members would be harmed by such theft.

131. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII/PHI that was collected and stored on their servers.

132. Fortra's duties to use reasonable security measures also arose as a result of the contractual relationship that existed between itself and NationsBenefits. Fortra knowingly agreed to provide NationsBenefits with software and services to facilitate

the transfer of PII/PHI, through which Fortra knowingly received Plaintiff's and the class members' sensitive information. Fortra therefore assumed a duty to act carefully and not put these individuals' information at an undue risk of harm, "by, for example, neglecting to implement data security policies and procedures." Fortra alone could have ensured that its software, security systems, and data storage architecture were sufficient to prevent or minimize the Data Breach.

133. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendants' duties.

134. Defendants' duty to use reasonable security measures also arose under HIPAA, under which Defendants were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

135. Defendants knew or should have known that NationsBenefits' GoAnywhere MFT server was vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII/PHI.

136. Defendants breached the duties they owed to Plaintiff and class members described above and thus were negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII/PHI of Plaintiff and class members; (b) detect the Breach while it was ongoing or even promptly after it occurred; and (c) maintain security systems consistent with industry standards.

137. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and class members, their PII/PHI would not have been compromised.

138. As a direct and proximate result of Defendants' negligence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 2
NEGLIGENCE *PER SE*
Against all Defendants

139. Plaintiff repeats and allege Paragraphs 1–126, as if fully alleged herein.

140. The Florida Information Protection Act of 2014 ("FIPA") requires "covered entities" like Defendants to "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. Ann. § 501.171(2).

141. Defendants are "covered entities" for the purposes of FIPA because it is a "commercial entit[ies] that acquire[], maintain[], store[], or use[] personal information." *Id.* at § 501.171(1)(b).

142. Defendants violated FIPA by failing to use reasonable measures to protect PII/PHI and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and quantity of PII/PHI obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

143. As a direct and proximate result of NationsBenefits' negligence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft

insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 4
DECLARATORY JUDGMENT
Against all Defendants

144. Plaintiff repeats and alleges Paragraphs 1–126, as if fully alleged herein.

145. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

146. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard their customers' PII/PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and class members from further data breaches that compromise their PII. Plaintiff remains at imminent risk that further compromises of their PII/PHI will occur in the future.

147. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' PII/PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, the Florida Information Protection Act, and various state statutes;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII/PHI.

148. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII/PHI

149. If an injunction is not issued, Plaintiff and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at NationsBenefits or Fortra. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

150. The hardship to Plaintiff and class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs at NationsBenefits or Fortra, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described

herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

151. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at NationsBenefits or Fortra, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose PII/PHI would be further compromised

COUNT 4
BREACH OF IMPLIED CONTRACT
Against NationsBenefits

152. Plaintiff repeats and alleges Paragraphs 1–126, as if fully alleged herein, and assert this claim in the alternative to their breach of contract claim to the extent necessary.

153. Plaintiff and class members also entered into an implied contract with NationsBenefits when they obtained services from NationsBenefits, or otherwise provided PII/PHI to NationsBenefits through their health insurance providers or employers.

154. As part of these transactions, NationsBenefits agreed to safeguard and protect the PII/PHI of Plaintiff and class members.

155. Plaintiff and class members entered into implied contracts with the reasonable expectation that NationsBenefits' data security practices and policies were

reasonable and consistent with industry standards. Plaintiff and class members believed that NationsBenefits would use part of the monies paid to NationsBenefits under the implied contracts to fund adequate and reasonable data security practices.

156. Plaintiff and class members would not have provided or entrusted their PII/PHI to NationsBenefits or would have paid less for NationsBenefits' services in the absence of the implied contract or implied terms between them and NationsBenefits. The safeguarding of the PII/PHI of Plaintiff and class members was critical to realize the intent of the parties.

157. Plaintiff and class members fully performed their obligations under the implied contracts with NationsBenefits.

158. NationsBenefits breached its implied contracts with Plaintiff and class members to protect their PII/PHI when it (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

159. As a direct and proximate result of NationsBenefits' breach of implied contract, Plaintiff and class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid and were overcharged by NationsBenefits for its services.

COUNT 5
UNJUST ENRICHMENT
Against NationsBenefits

160. Plaintiff repeats and alleges Paragraphs 1–126, as if fully alleged herein.

161. Plaintiff and class members have an interest, both equitable and legal, in the PII/PHI that was conferred upon, collected by, and maintained by NationsBenefits and that was ultimately stolen in the Data Breach.

162. NationsBenefits benefitted from the conferral upon it of the PII/PHI pertaining to Plaintiff and class members and from its ability to retain, use, and profit from that information. NationsBenefits understood that they were in fact so benefitted.

163. NationsBenefits also understood and appreciated that the PII/PHI pertaining to Plaintiff and class members was private and confidential and its value depended upon NationsBenefits maintaining the privacy and confidentiality of that PII/PHI.

164. But for NationsBenefits' willingness and commitment to maintain its privacy and confidentiality, that PII/PHI would not have been transferred to and entrusted with NationsBenefits.

165. NationsBenefits continued to benefit and profit from their retention and use of the PII/PHI while its value to Plaintiff and class members has been diminished.

166. NationsBenefits also benefitted through its unjust conduct by retaining portions of Plaintiff's and the class members' monthly premiums that it should have used to provide reasonable and adequate data security to protect Plaintiff' and class members' PII.

167. It is inequitable for NationsBenefits to retain these benefits.

168. As a result of NationsBenefits' wrongful conduct as alleged in this Complaint (including, among things, their knowing failure to employ adequate data security measures, their continued maintenance and use of the PII/PHI belonging to Plaintiff and class members without having adequate data security measures, and their other conduct facilitating the theft of that PII), NationsBenefits has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and class members.

169. NationsBenefits' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and class members' PII/PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

170. Under the common law doctrine of unjust enrichment, it is inequitable for NationsBenefits to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiff and class members in an unfair and unconscionable manner. NationsBenefits' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

171. The benefits conferred upon, received, and enjoyed by NationsBenefits was not conferred officiously or gratuitously, and it would be inequitable and unjust for NationsBenefits to retain these benefits.

172. Plaintiff has no adequate remedy at law.

173. NationsBenefits is therefore liable to Plaintiff and class members for restitution or disgorgement in the amount of the benefit conferred on it as a result of

its wrongful conduct, including specifically: the value to NationsBenefits of the PII/PHI that was stolen in the Data Breach; the profits NationsBenefits receives from the use of that information; the amounts that Plaintiff and class members were overcharged for their health insurance or supplemental benefits insurance as a result of NationsBenefits' services; and the amounts that NationsBenefits should have spent to provide reasonable and adequate data security to protect Plaintiff's and class members' PII/PHI.

COUNT 6

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, et seq.

Against NationsBenefits

174. Plaintiff repeats and allege Paragraphs 1–126, as if fully alleged herein.

175. Plaintiff and Class members are "consumer[s]" as defined by Fla. Stat. § 501.203.

176. NationsBenefits advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

177. NationsBenefits engaged in unconscionable and unfair acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

178. As a direct and proximate result of NationsBenefits' unconscionable, unfair, and deceptive acts and practices, Plaintiff and class members have suffered actual damages, through the diminution in the value of the supplemental benefits administration services that NationsBenefits provides to them through their health insurance providers. Plaintiff would not have paid for, or would have paid less for, NationsBenefits' supplemental benefits administration had they known about its failure to comply with HIPAA and other statutes, as well as with reasonable security standards.

179. In addition, Plaintiff and class members have suffered and will continue to suffer damages, including the injury, ascertainable losses of money or property, and monetary and non- monetary damages, including loss of the benefit of their bargain with and overcharges by NationsBenefits, as they would not have paid NationsBenefits for services or would have paid less for such services but for the violations alleged

herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

180. Plaintiff and class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 7
DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT

Texas Bus. & Com. Code §§ 17.41, et seq.
Against All Defendants

181. Plaintiff, individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1–126, as if fully alleged herein.

182. Defendants are "person[s]" as defined by Tex. Bus. & Com. Code § 17.45(3).

183. Plaintiff and the Texas Subclass are "consumer[s]" as defined by Tex. Bus. & Com. Code § 17.45(4).

184. Defendants advertised, offered, or sold services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

185. The Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). The Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

186. Consumers, including Plaintiff and Texas Subclass, lacked knowledge about deficiencies in the Defendant' data security because this information was known exclusively by the Defendant. Consumers also lacked the ability, experience, or capacity to secure the PII/PHI in the Defendant' possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass members lack expertise in information security matters and do not have access to the Defendant' systems in order to evaluate their security controls. The Defendants took advantage of their special skill and access to the PII/PHI to hide their inability to protect the security and confidentiality of Plaintiff and Texas Subclass members' PII/PHI.

187. The Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from the Defendant' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from the Defendants' unconscionable business acts and practices, exposed Plaintiff and Texas Subclass members to a wholly unwarranted risk to the safety of their PII/PHI and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff

and Texas Subclass members cannot mitigate this unfairness because they cannot undo the Data Breach.

188. The Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff's and the Texas Subclass' rights. Defendants are of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

189. As a direct and proximate result of the Defendants' unconscionable and deceptive acts or practices, Plaintiff and the Texas Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with and overcharges by NationsBenefits, as they would not have paid NationsBenefits for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII/PHI; and an increased, imminent risk of fraud and identity theft.

190. The Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiff's and Texas Subclass' injuries, ascertainable losses and economic and non-economic damages.

191. The Defendants' violations present a continuing risk to Plaintiff and Texas Subclass members as well as to the general public.

192. Plaintiff and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; treble damages for each act committed intentionally or knowingly; restitution; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and Plaintiff's Lead Counsel to represent the classes as alleged herein;

b. For injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and class members, including but not limited to an order:

c. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

d. Requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

e. Requiring Defendants to delete, destroy and purge the PII/PHI of Plaintiff and class members unless NationsBenefits can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and class members;

f. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff' and class members' PII/PHI;

g. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

h. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

i. Requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

j. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is

compromised, hackers cannot gain access to other portions of Defendants' systems;

k. Requiring Defendants to conduct regular database scanning and securing checks;

l. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Plaintiff and class members;

m. Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

n. Requiring Defendants to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting PII/PHI;

o. Requiring Defendants to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor the Defendants' information networks for threats, both internal

and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

p. Requiring Defendants to meaningfully educate all class members about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps affected individuals must take to protect themselves;

q. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

r. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

s. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

t. For an award of statutory damages, trebled, and punitive or exemplary damages, as allowed by law in an amount to be determined;

u. For an award of restitution or disgorgement, in an amount to be determined;

v. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

w. For prejudgment interest on all amounts awarded; and

x. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: June 7, 2023

PLAINTIFF, individually and on behalf of all others similarly situated,

/s/ Avi R. Kaufman

Avi R. Kaufman (FL Bar no. 84382)*
kaufman@kaufmanpa.com
Rachel E. Kaufman (FL Bar no. 87406)
rachel@kaufmanpa.com
KAUFMAN P.A.
237 South Dixie Highway, 4th Floor
Coral Gables, FL 33133
Telephone: (305) 469-5881

*Trial Counsel

Counsel for Plaintiff and the putative Class